Latest Cyber Security Techniques and Trending

Agenda

- Cyber Security Techniques and Trending
  - Ransomware
  - Fileless Threats
  - Cryptocurrency-mining Malware
  - Messaging Threats
  - High-Impact Vulnerabilities
  - IoT and IIoT Attacks
- Recommendation and Conclusion

Ransomware

A persistent and far-reaching threat, ransomware continued to be costly for businesses.

Cybercriminals were more selective in their targets, focusing on:

- Multinationals
- Large enterprises
- Government organizations

There were several high-profile ransomware attacks in the first six months of 2019, including ones that affected a Norwegian manufacturing company and local government organizations in Florida, Maryland, and North Carolina.

Ransomware operators compromised mission-critical systems, thereby affecting organizations' operations and bottom lines.

*From the second half of 2018 to the first half of 2019

77%

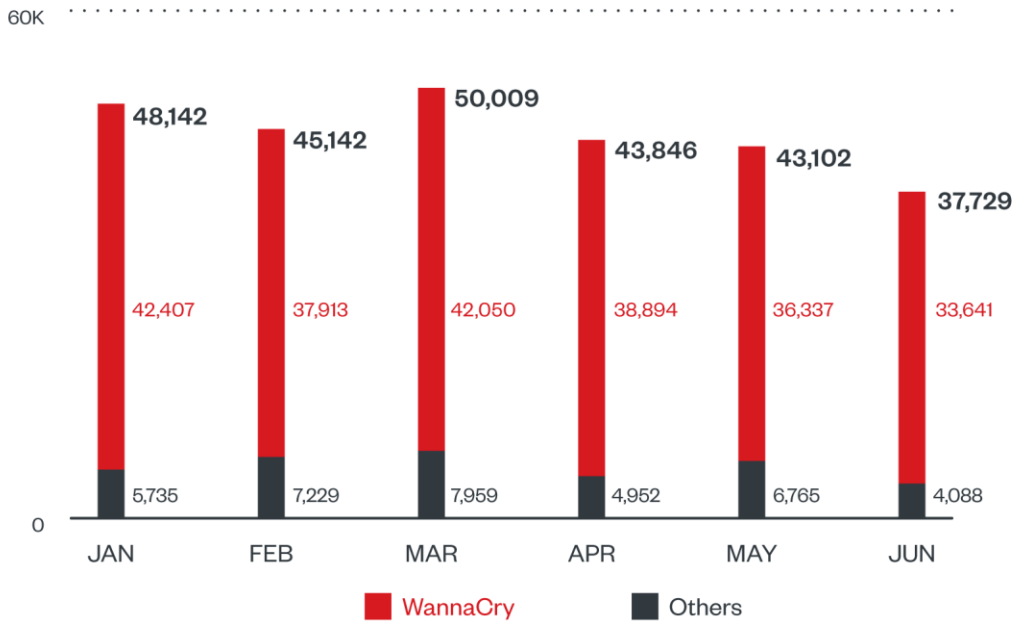
Increase in overall ransomware detections*

55%

Decrease in new ransomware families*

WannaCry still reigns supreme

- Despite having been patched since 2017, WannaCry still accounted for the majority of ransomware detections in the first half of 2019
- Most detections were from systems running Windows 7



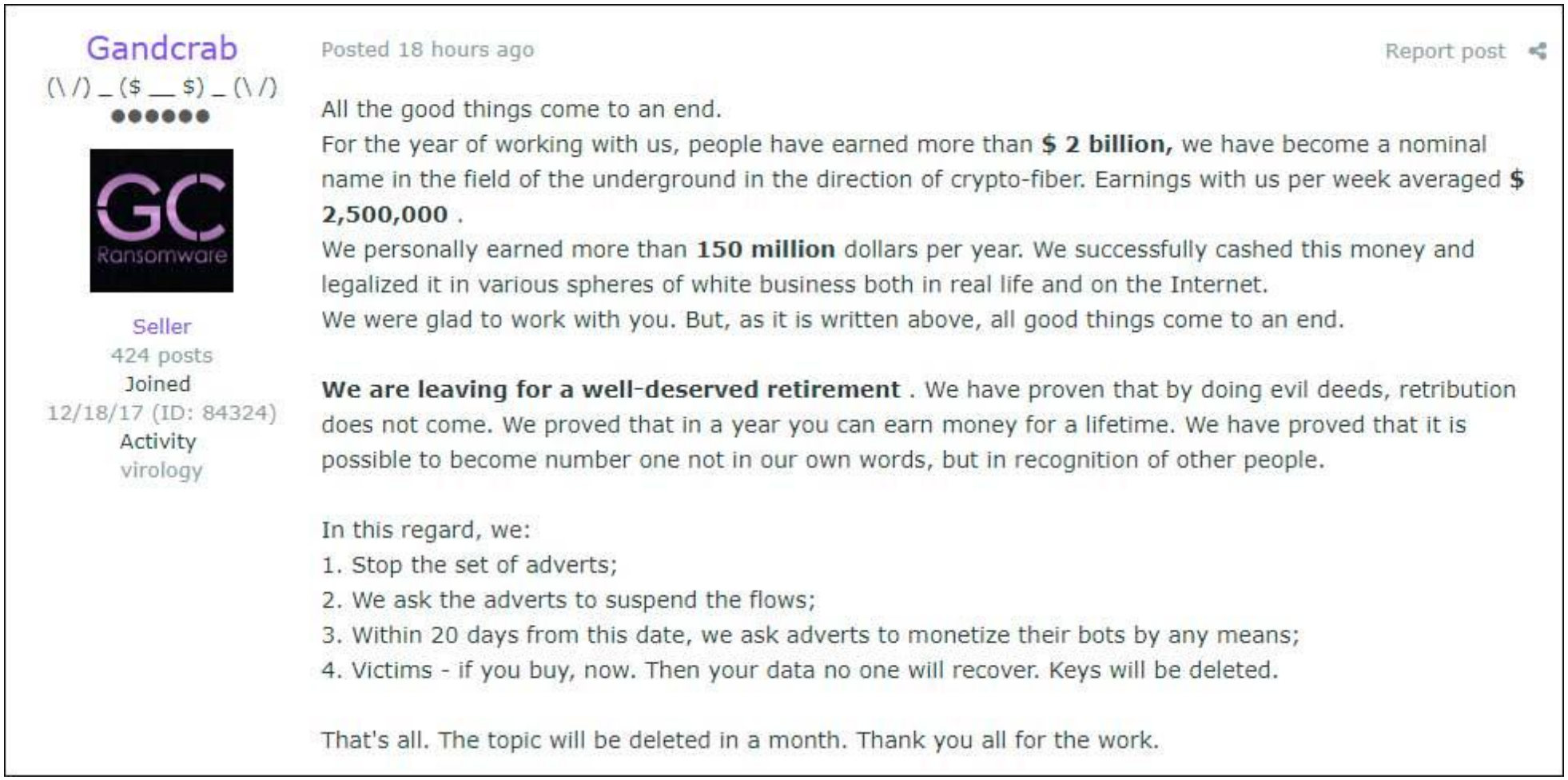
Comparison between detections of WannaCry and combined detections of the other ransomware families in the first half of 2019

Distribution of WannaCry detections in the first half of 2019 by operating system

GandCrab

- Earned over 2 billion
- Has stopped
  - 2018/01 – 2019/06
- RaaS - Ransomware as a Service

GrandCrab Announcement



Gandcrab

(\ /) _ ($ __ $) _ (\ /)

Seller
424 posts
Joined
12/18/17 (ID: 84324)
Activity
virology

Posted 18 hours ago

Report post

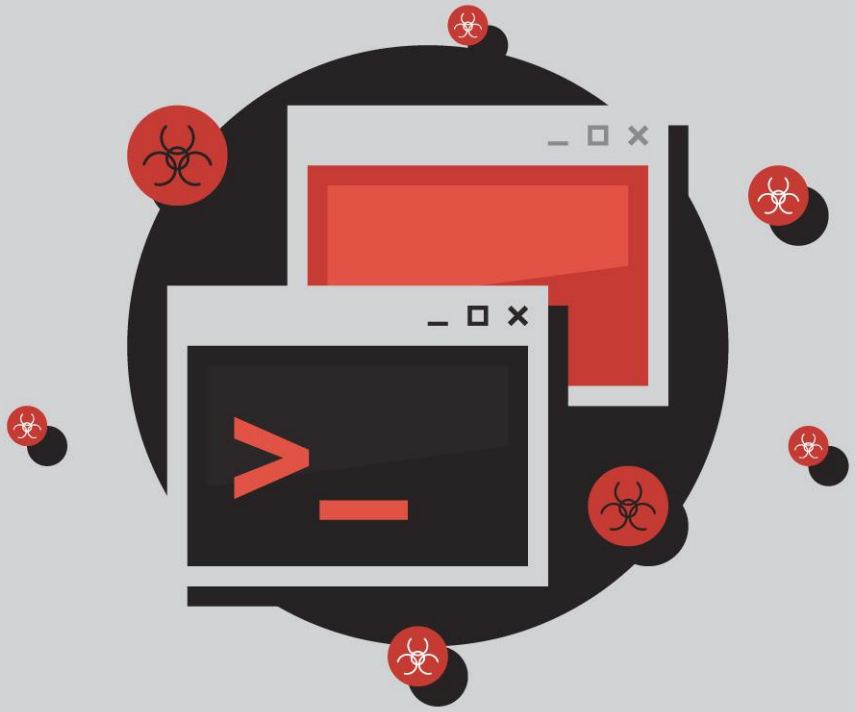
All the good things come to an end.
For the year of working with us, people have earned more than **$ 2 billion,** we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **$ 2,500,000** .
We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:
1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

From: Bleeping Computer - GandCrab Ransomware Shutting Down After Claiming to Earn $2 Billion

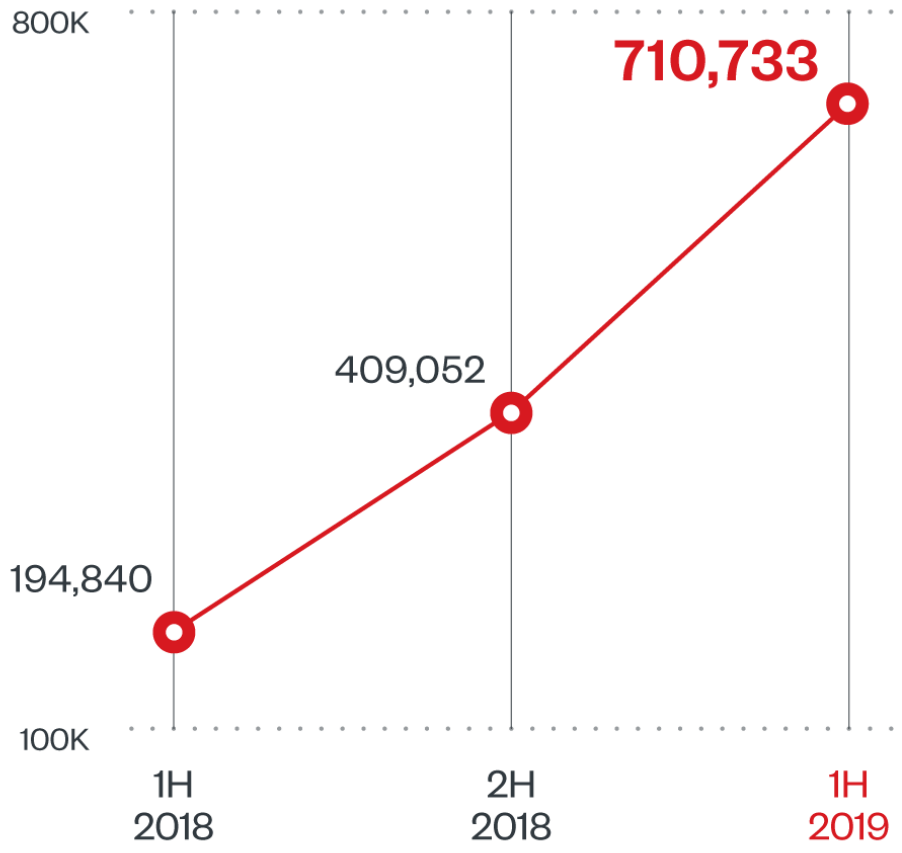


Threats that ‘live off the land’

Threat actors increasingly abused legitimate tools or whitelisted applications.

Fileless threats

As we predicted, threat actors had been “living off the land,” abusing or repurposing legitimate system administration or penetration testing tools to blend in.



Half-year comparison of fileless events blocked

Notable threats that used fileless techniques to drop or execute their payloads:

- Cryptocurrency-mining malware
- Ransomware
- Banking trojans

These threats all abused PowerShell.

There was **a steep rise in fileless events detected in the first half of 2019**.

603.9k

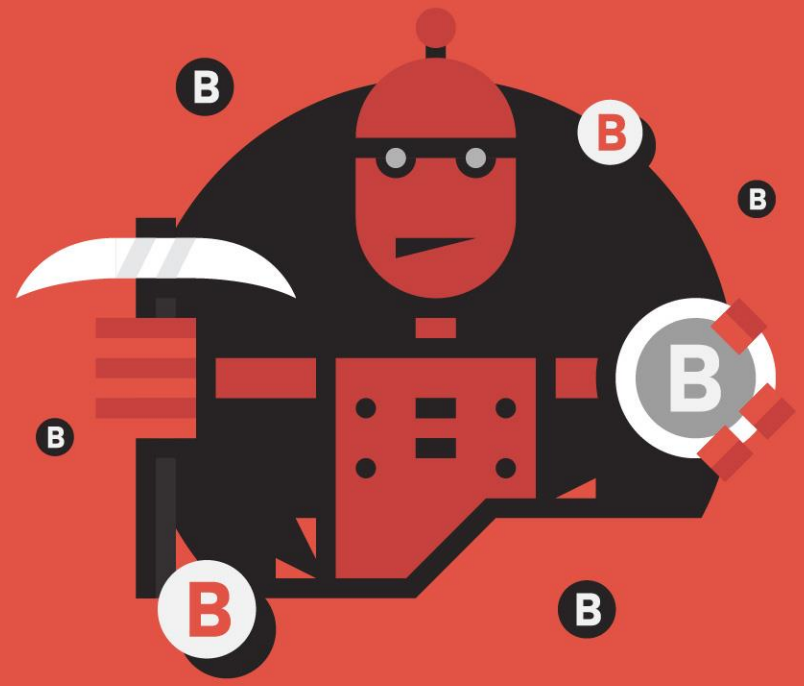
All of 2018

710.7k

First half of 2019

Protection against fileless threats

Enterprises need to implement proactive security measures. They should practice defense in depth, where multilayered safeguards are placed to reduce exposure and mitigate damage.

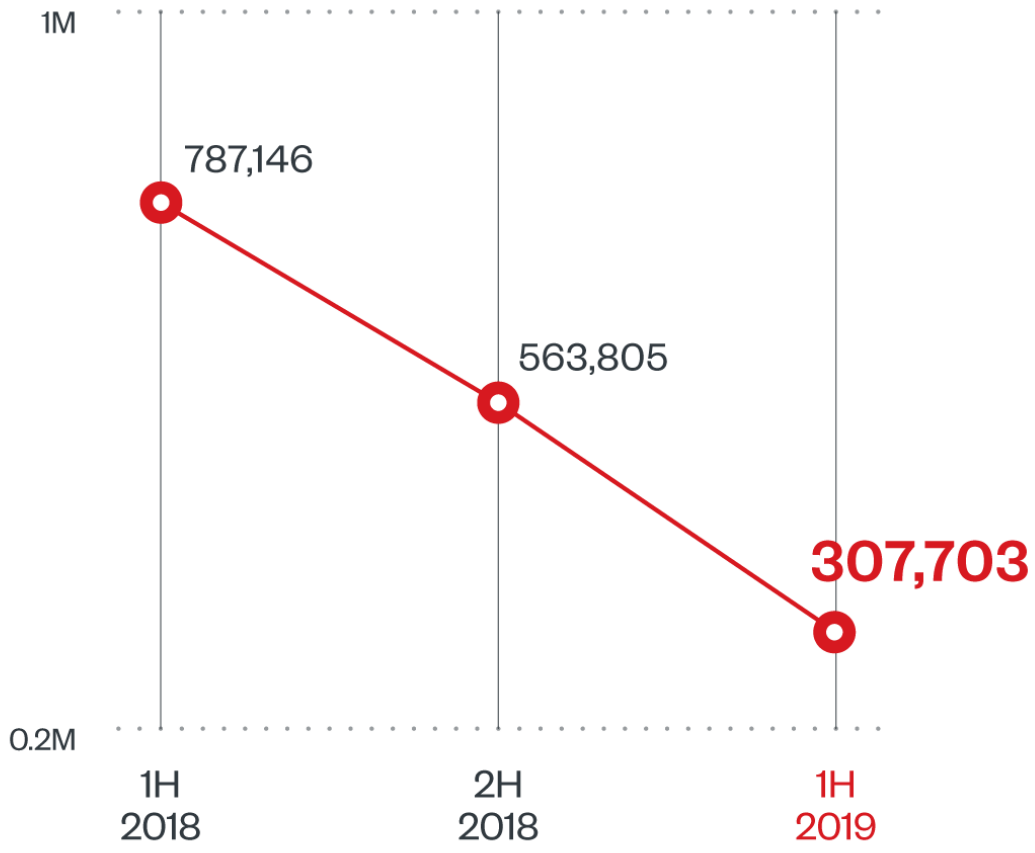


Cryptocurrency-mining malware

Illicit cryptocurrency miners looked for more effective methods and resources.

Cryptocurrency-mining malware was still the most detected threat (file-based) in the first half of 2019, although overall detections continued to decline since 2018.

This threat adopted tools normally associated with targeted attacks or information theft campaigns, like advance hacking tools and modular malware.



Half-year comparison of detections of file-based cryptocurrency-mining malware-related threat components

Cryptocurrency-mining malware was deployed on servers and, as we predicted, in cloud environments.

Devices or endpoints cannot deliver the nearly unlimited resources cloud infrastructures can provide. For cybercriminals, unguarded or unsecured assets such as those are prime targets.

Protection against cryptocurrency-related threats

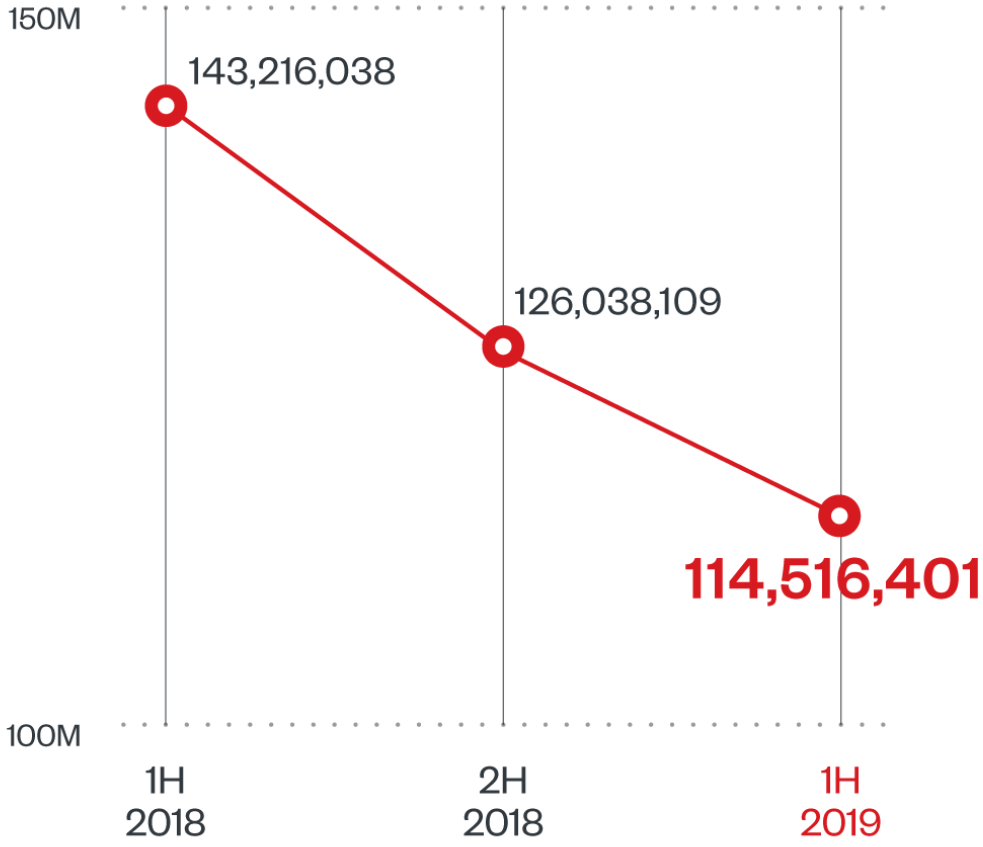
Given cryptocurrency-mining threats' increased sophistication of routines and broadening scale of deployment, having greater visibility and control over systems can help organizations better identify the activities and processes running in their online infrastructures.

Messaging threats

A diverse number of threats entered enterprise networks through communication tools and applications

Phishing

Phishing activities decreased in the first half of 2019. From the second half of 2018, there was **a 9% drop in instances of blocked access to non-unique phishing-related URLs**.

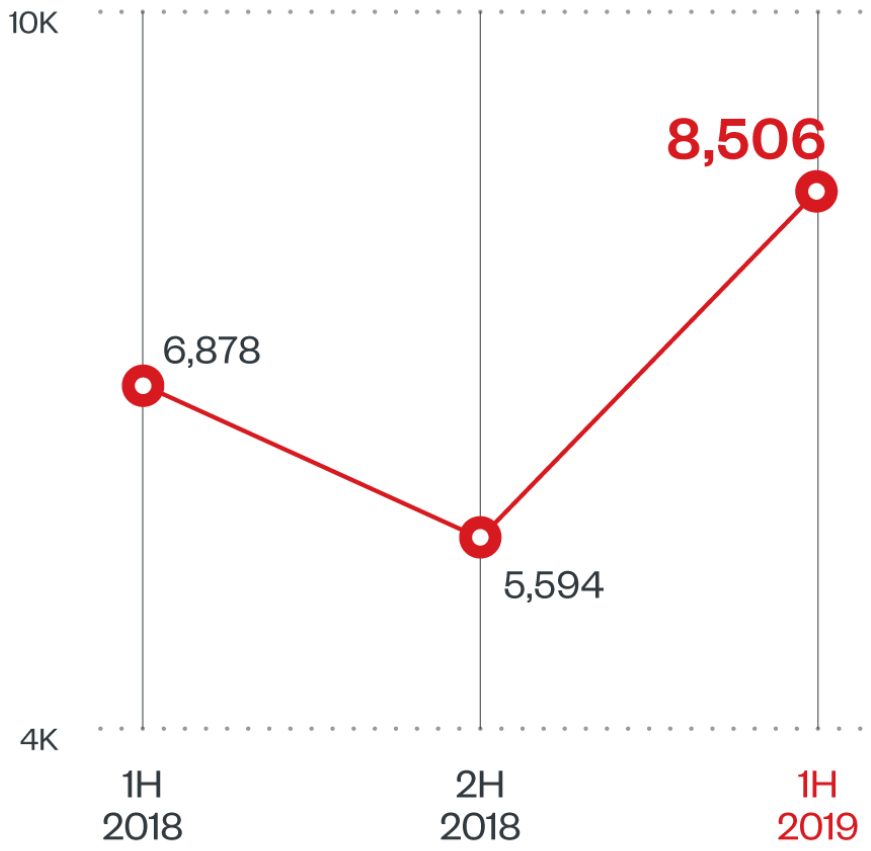


Half-year comparison of instances of blocked access to non-unique phishing URLs (e.g., three instances of blocked access to the same URL counted as three)

Business email compromise

Business email compromise (BEC) attempts thrived well into the first half of 2019, increasing by 52% from the second half of 2018.

The CEO remained the most spoofed position, accounting for 40% of BEC attempts in the first half of 2019.

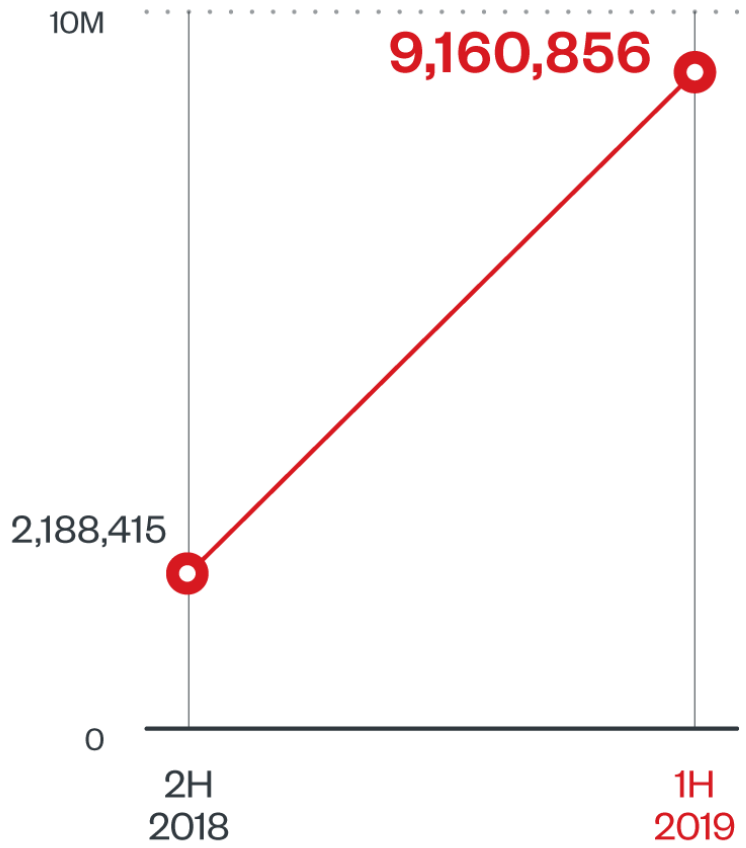


Half-year comparison of BEC attempts

Sextortion

We predicted that **in 2019 there would be an increase in instances of digital extortion, particularly sextortion**.

There was **a 319% increase in detections of sextortion-related spam emails** compared to the second half of 2018.



Half-year comparison of detections of sextortion-related spam emails

Sextortion Example

Hello!

I have very bad news for you.
21/05/2019 - on this day I hacked your OS and got full access to your account [redacted]

So, you can change the password, yes... But my malware intercepts it every time.

How I made it:
In the software of the router, through which you went online, was a vulnerability.
I just hacked this router and placed my malicious code on it.
When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $723 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!
My BTC wallet: 1Lkdmscmiuj1nRVxCkYBx93fFL52idYTuH

You do not know how to use bitcoins?
Enter a query in any search engine: "how to replenish btc wallet".
It's extremely easy

For this payment I give you two days (48 hours).
As soon as this letter is opened, the timer will work.

After payment, my virus and dirty screenshots with your enjoys will be self-destruct automatically.
If I do not receive from you the specified amount, then your device will be locked, and all your contacts will receive a screenshots with your "enjoys".

I hope you understand your situation.
- Do not try to find and destroy my virus! (All your data, files and screenshots is already uploaded to a remote server)
- Do not try to contact me (this is impossible, sender's address was randomly generated)
- Various security services will not help you; formatting a disk or destroying a device will not help, since your data is already on a remote server.

P.S. You are not my single victim. so, I guarantee you that I will not disturb you again after payment!
This is the word of honor hacker

I also ask you to regularly update your antiviruses in the future. This way you will no longer fall into a similar situation.

Do not hold evil! I just do my job.
Have a nice day!

Sextortion Example

Hello!

I have very bad news for you.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

I know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $723 is a very, very small amount for my silence.

Pay ONLY in Bitcoins!
My BTC wallet: 1Lkdmscmiuj1nRVxCkYBx93fFL52idYTuH

P.S. You are not my single victim. so, I guarantee you that I will not disturb you again after payment!
This is the word of honor hacker

I also ask you to regularly update your antiviruses in the future. This way you will no longer fall into a similar situation.

Do not hold evil! I just do my job.
Have a nice day!

Protection against messaging threats

Organizations need an enhanced cybersecurity defense to stop attackers who continue to cast wider phishing nets. Cybersecurity awareness is also essential in keeping organizations safe from cyberattacks: Employers have to build awareness in employees to help them identify such attacks.

High-Impact Vulnerabilities

Pervasive vulnerabilities highlighted the need for enterprise patching.

The majority of the vulnerabilities reported through our Zero Day Initiative (ZDI) program were **rated high in severity**.

LOW (0.1-3.9)	107
MEIDUM (4.0-6.9)	101
HIGH (7.0-8.9)	**335**
CRITICAL (9.0-10.0)	40

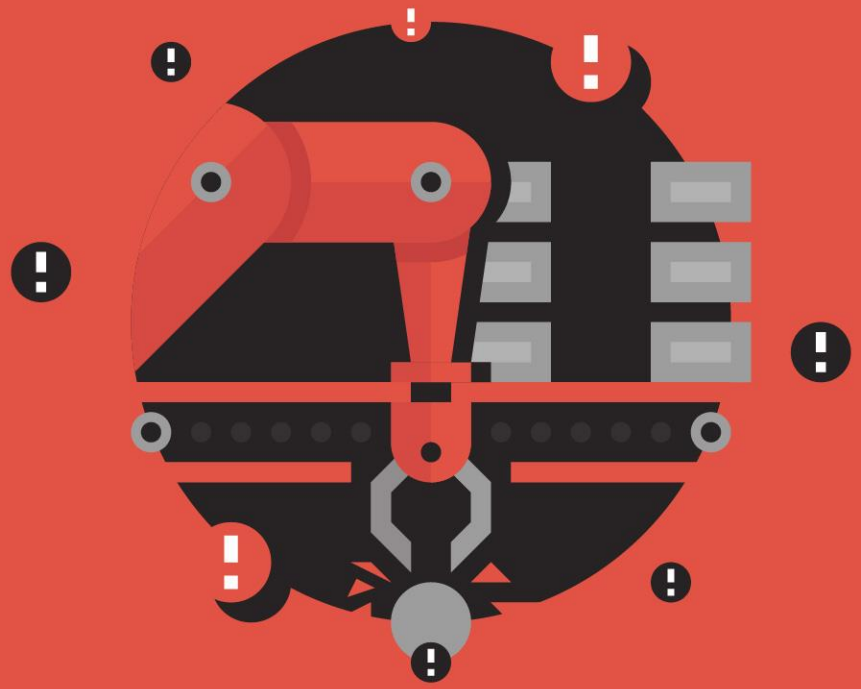
Severity breakdown, based on Common Vulnerability Scoring System (CVSS) v3.0, of vulnerabilities disclosed in the first half of 2019 through our Zero Day Initiative (ZDI) program

There were severe and pervasive **vulnerabilities that could heavily impact enterprises if exploited**.

VULNERABILITY	NOTABLE BEHAVIOR
CVE-2019-0708 Aka BlueKeep, a critical vulnerability in remote desktop services	Can give malware extreme propagation capabilities
CVE-2019-1069 A vulnerability in Windows 10's Task Scheduler	Can allow hackers to access protected files
CVE-2019-5736 A vulnerability in runC, a runtime component used for container platforms	Can give hackers full control of the host running an affected container
CVE-2019-1002101 A vulnerability in Kubernetes' command-line interface for running commands and managing resources	Can push users into downloading malicious container images
CVE-2019-9580 A vulnerability in the workflow automation tool StackStorm	Can expose servers to unauthorized access

Protection against vulnerability exploits

Organizations should stay vigilant and stay ahead of critical vulnerabilities through effective patching routines. Malicious actors repurpose exploits for old and patched vulnerabilities, and take advantage of windows of exposure.



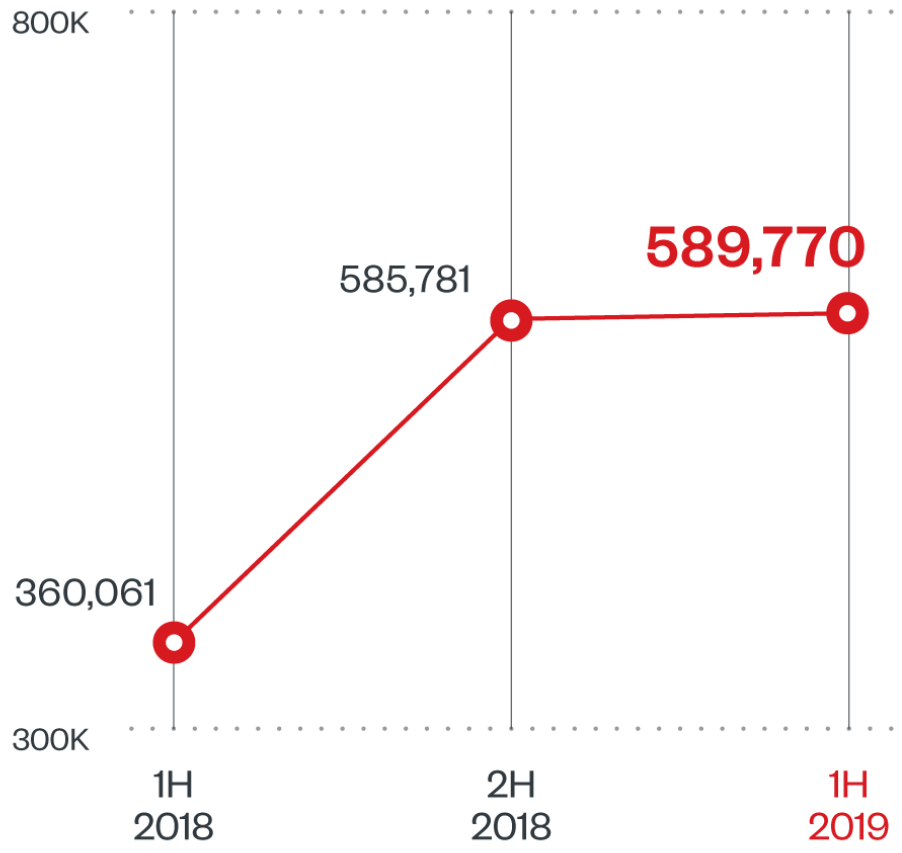
IoT and IIoT attacks

The continued proliferation of the IoT and IIoT across enterprise fields and the continued development of new attacks underscored the importance of security.

The internet of things

Threat actors capitalized on improper configuration and other forms of weak security in IoT devices.

Our data showed a considerable number of routers involved in possible inbound attacks (attacks coming from the internet to the routers and devices connected to them).

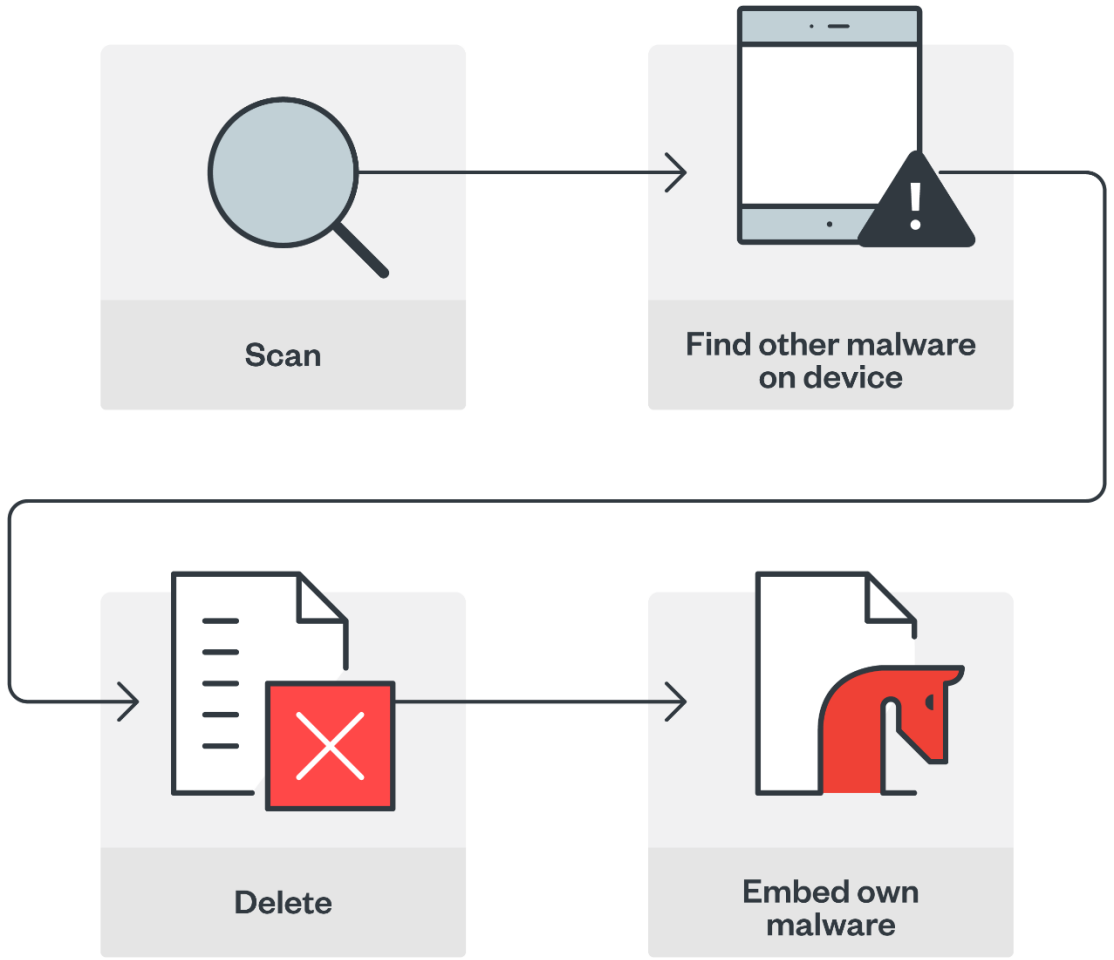


Half-year comparison of routers identified to have been involved in possible inbound attacks

As we predicted, the IoT landscape had become **a battleground of botnets and worms vying for control over their infected devices**.

The players: Bashlite, Mirai variants such as Omni, Hakai, and Yowai

The routine: scanning the infected device for any competing malware or payload already in the device, deleting it, and embedding their own



The industrial internet of things

The IIoT is deeply integrated into critical infrastructures and many large-scale enterprises need these machines to operate.

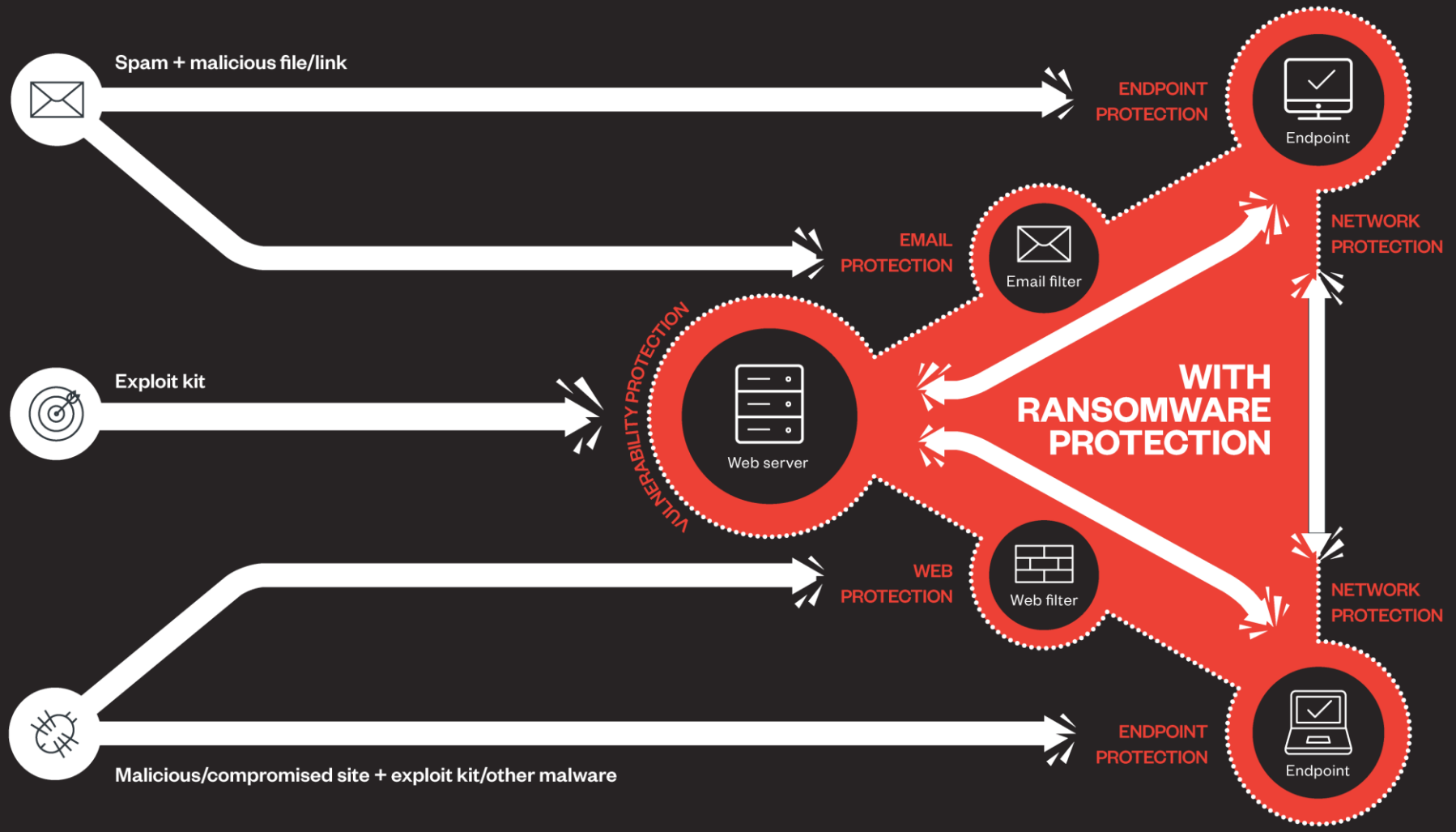
In the first half of 2019, malicious actors seemed to be assessing IIoT targets: The Xenotime hacking group was seen probing the ICSs of power grids in the U.S. and Asia-Pacific region. **Its malware scanned for and listed its targets' remote login portals and vulnerabilities in their networks**.

Protection against IoT- and IIoT-related threats

IoT and IIoT devices are found in homes, workplaces, and entire industries. The security risks to these devices will persist as long as their users and manufacturers continue to forgo something as simple as changing or updating device credentials.

Multilayered defense helps address today’s multifaceted threats

Layered protection against ransomware



Thank You All

- Chia-Ching Fang
  - vico_fang@trendmicro.com
  - @0xvico